IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

IN THE MATTER OF THE CIVIL FORFEITURE OF 3.0103 BTC, 1.0017 ETH, AND 372,516.27 USDT, ASSOCIATED WITH BINANCE USER ID 26257660 IN THE NAME OF OGAGA MICHAEL PANAMA	Case No. 6:22-CV-

AFFIDAVIT IN SUPPORT OF CIVIL FORFEITURE

I, Michael Dawson, after being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service (USSS or Secret Service). I am stationed in Tyler, Texas, and have been a Special Agent for over twenty years. During my tenure with the Secret Service, I have been assigned to investigate violations of federal laws, including violations of Title 18 of the United States Code, and specifically those related to the passing of counterfeit United States currency and wire fraud. I received criminal investigative training at the Federal Law Enforcement Training Center in Glynco, Georgia, and at the James J. Rowley Secret Service Training Center in Beltsville, Maryland, pertaining to criminal investigations of counterfeit currency, bank fraud, money laundering, wire fraud, access device fraud, and identity theft. During my employment with the USSS, I have conducted investigations resulting in the arrest of suspects and seizures of criminally derived property. I am an investigative and law enforcement officer of the United States, in that I am empowered by law to conduct

investigations and to make arrests for felony offenses, under authority of 18 U.S.C. § 3056.

2. The statements contained in this affidavit are based in part upon my experience, my knowledge of the facts and circumstances surrounding this investigation, and on information provided to me by other law enforcement personnel and other witnesses. This affidavit does not set forth all of my knowledge about this matter.

PROPERTY TO BE FORFEITED

3. This affidavit is made to obtain the civil forfeiture of 3.0103 BTC, 1.0017 ETH, and 372,516.27 USDT, associated with Binance user ID 26257660 in the name of Ogaga Michael Panama ("PANAMA") (hereinafter collectively referred to as the "Seized Property").

LEGAL AUTHORITY FOR SEIZURE

4. Based on my experience and the information contained in the subsequent paragraphs, I have probable cause to believe that this property is subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) because the property was involved in or traceable to property involved in money laundering in violation of 18 U.S.C §§ 1956 or 1957.

5. Any property, real or personal, which was involved in a transaction in violation of 18 U.S.C. §§ 1956 or 1957 or any property traceable to such property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

6. Title 18 U.S.C. § 1956(a)(1) makes it a crime to knowingly conduct or attempt to conduct a "financial transaction" with proceeds from "specified unlawful activity" ("SUA") with specific intent to: promote the SUA, conceal or disguise the source, origin, nature, ownership, or control of the proceeds; evade reporting requirements; or evade taxes.

7. The purpose of "money laundering" as defined by 18 U.S.C. § 1956 is to disguise illicit nature of funds by introducing it into legitimate commerce and finance thereby making them "clean." This financial process is most commonly conducted using three steps referred to as "placement," "layering," and "integration." Typically, the "placement" phase of this financial process takes place when proceeds from illicit sources are placed in a financial institution or business entity. "Layering" takes place when these funds are then used in seemingly legitimate commerce transactions which makes the tracing of these monies more difficult and removed from the criminal activity from which they originated. Finally, the "integration" phase is when these funds are then used to promote the unlawful activity or for the personal benefit of the money launderers and others.

8. I also have probable cause to believe that this property is subject to seizure and forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) because the property constitutes or is derived from proceeds traceable to violations of 18 U.S.C. §§ 1341 (mail fraud) and/or 1343 (wire fraud) or a conspiracy to commit such offenses.

9. Any property, real or personal, which constitutes proceeds or is derived from proceeds traceable to a violation of 18 U.S.C. §§ 1341 and/or 1343 or a conspiracy to commit such is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

10. The property is subject to seizure via a civil seizure warrant under 18 U.S.C. §§ 981(a) and 981(b).

11. Under 18 U.S.C. § 984, for any forfeiture action in rem in which the subject property consists of cash, monetary instruments in bearer form, or funds deposited in an account in a financial institution:

a. The government need not identify the specific funds involved in the offense that serves as the basis for the forfeiture;

b. It is not a defense that those funds have been removed and replaced by other funds; and

c. Identical funds found in the same account as those involved in the offense serving as the basis for the forfeiture are subject to forfeiture.

12. In essence, 18 U.S.C. § 984 allows the government to seize for forfeiture identical property found in the same place where the "guilty" property had been kept. The statute does not, however, allow the government to reach back in time for an unlimited period. A forfeiture action (including a seizure) against property not directly traceable to the offense that is the basis for the forfeiture cannot be commenced more than one year from the date of the offense.

13. Funds in a bank are fungible, thus making them subject to transfer or withdrawal with relative ease. Furthermore, I know that once U.S. Currency is converted to cryptocurrency, the funds become difficult to recover and trace. A restraining order would be inadequate to preserve property of this type for forfeiture at trial. Based on my training and experience, I know that restraining orders served on banks sometimes fail to preserve the property for forfeiture because the bank representative receiving the restraining order fails to put the necessary safeguards in place to freeze the money in time to prevent the account holder from accessing the funds electronically, or fails to notify the proper personnel as to the existence of the order, or the bank exercises its own right of setoff to satisfy an outstanding debt owed to the bank by the account holder. In contrast, where electronic funds are concerned, a seizure warrant guarantees that the funds will be in the government's custody upon execution of the warrant and, thus, preserved for forfeiture at trial.

BACKGROUND ON CRYPTOCURRENCY

14. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. Cryptocurrency, a type of digital currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other

cryptocurrencies.[1] Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[2] Cryptocurrency is not illegal in the United States.

b. Bitcoin[3] ("BTC") is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals

[1] Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

[2] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

[3] Because Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a bitcoin. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. BTC transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it is not completely anonymous, BTC allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

c. Ethereum ("ETH") and Tether ("USDT") are also types of cryptocurrencies.

d. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26–25 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

e. Although cryptocurrencies such as BTC have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering, and is an oft-used means of payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transactions. As of January 19, 2022, one BTC was worth approximately

$42,100.00, though the value of BTC is generally much more volatile than that of fiat currencies.

f. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (*e.g.*, Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[4] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a

[4] A QR code is a matrix barcode that is a machine-readable optical label.

complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

g. BTC "exchangers" and "exchanges" are individuals or companies that exchange bitcoin for other currencies, including U.S. dollars. According to Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[5] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to

[5] *See* "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," *available at* https://www.fincen.gov/resources/statutes-regulations/guiadance/application-fincens-regulations-persons-administering.

provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

h. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users'

cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

i. BTC is commonly the cryptocurrency of choice for fraud schemes because it is easily obtained by victims and easily converted by suspects. Once BTC is received by the suspects, it is often exchanged for ETH. One reason for this exchange, known as chain hopping, is that it allows suspects to take the cryptocurrency off of the BTC blockchain and move it to the ETH blockchain in an effort to conceal the location, nature, and source of the proceeds. Additionally, cryptocurrency exchangers, prefer to possess ETH for those customers who wish to exchange BTC or other tokens for ETH. ETH is also typically less volatile than BTC.

FACTS SUPPORTING CIVIL FORFEITURE

Investigation Background

15. This investigation has revealed that the account held under user ID 36702473 at Binance, a cryptocurrency exchange, in the name of Ogaga Michael PANAMA received proceeds from various methods of mail and wire fraud schemes within the United States.

16. By way of background, I have learned through my training and experience that there are many different types of mail and wire fraud schemes, such as romance scams, lottery scams, Social Security scams, and advance payment fee scams, among others. The mail and wire fraud schemes rely on unsuspecting victims to utilize various types of financial accounts in order to conduct financial transactions that facilitate the fraud schemes. Depending on the "fraud story," the victims are led to believe that they need to send money in order to receive a larger sum of money or other form of benefit such as a romantic relationship. Often, the initial transactions are in small amounts and are designed to gain the victim's trust. Subsequent transactions are often in larger amounts and cause financial loss to the victim. The goal of these mail and wire fraud schemes, described herein, is to steal money from the victims through fraud and deceit.

The transactional flow of victims' funds is shown through the money laundering process.

17. This investigation has identified multiple individuals, both domestic and foreign, who have conspired to defraud victims through various mail and wire fraud schemes such as romance scams, rent scams, and advance payment fee schemes. The victims are often instructed by foreign actors to send their money to other participants in the schemes in various ways, including cash by mail, wire/ACH transactions, credit/debit card platforms, and cash deposits.

18. Victim funds are usually sent to individuals referred to as domestic processors or money mules, who accept fiat currency from the victims or other domestic processors and exchange fiat currency for cryptocurrency. Cryptocurrency can be acquired quickly and can be transferred to foreign actors within minutes. The transactions are often difficult to identify and trace, and victim funds are rarely recoverable. Additionally, participants in these schemes are often able to evade detection and maintain a level of anonymity due to the nature of cryptocurrency.

Law enforcement identifies Diana Johnson as a suspect in a mail and wire fraud and money laundering scheme.

19. During the investigation, CI#19-2002[6] conducted 42 separate transactions with Localbitcoins user "Dianalj" between September 2019 to July 2020. During initial transactions, user "Dianalj" was required by CI#19-2002 to provide a photograph of her

[6] CI#19-2002 is a source who resided and operated along with USSS agents within the Eastern District of Texas.

identification. User "Dianalj" sent CI#19-2002 a photograph of a Florida state driver's license bearing the name Diana Lynn Fenton-Johnson and an address in Valrico, Florida. This identification was confirmed via NCIC database search. Bank records for transactions in the operation included security video and photographs. The security photographs captured a female subject making deposits. The individual making deposits in the security photograph was the same individual featured on the Florida driver's license provided by "Dianalj." User "Dianalj" was identified as Diana Lynn Fenton-Johnson.

20. Security photographs captured an individual assisting Fenton-Johnson in depositing cash in bank accounts held and controlled in the Eastern District of Texas. NCIC database records identified Roger Johnson as an emergency contact for Diana Lynn Fenton-Johnson. The individual making deposits with Fenton-Johnson was the same individual identified in NCIC database records and featured in the Florida's driver's license database for Roger Johnson.

21. Information obtained from United States Postal Service and Federal Express reflect that Fenton-Johnson and Roger Johnson received mail and packages at an address in Valrico, Florida from May 2019 through April 2020.[7] In total, approximately 83 U.S. Postal Service parcels and 33 Federal Express parcels were reportedly sent to the Johnson's Valrico address between May 2019 and April 2020.

[7] The address where packages were received was the same address shown on Fenton-Johnson's Florida state driver's license.

22. Records for the suspicious packages were reviewed, including the sender's address. From May 2019 through April 2020, there were approximately 15 fraudulent packages identified. The total dollar value for the mentioned packages was $34,750.00; $5,100.00 dollars was intercepted and returned to senders. The senders of the packages were contacted by law enforcement officers and reported their reasons for sending cash and other forms of financial tender in the mail. The reasons provided included information about romance scams, grant payment scams, lottery scams, and Social Security scams.

Romance Scam Victim S.G.

23. On November 21, 2019, a co-conspirator caused victim S.G. to send $500.00 in cash via Federal Express to Diana Johnson at her address in Valrico, Florida. The money arrived on November 22, 2020.

24. On November 22, 2019, Diana Johnson and her co-conspirators negotiated a trade of BTC with CI#19-2002 for a counter deposit of $1,500 into bank accounts controlled within the Eastern District of Texas and directed the BTC to be deposited into 13HW9yMGeEtC9JCgn8spPsPYEWK4qBZvb1 ("13HW").

25. Law enforcement officers contacted victim S.G. Between November 2019 and February 2020, S.G. sent three packages to Diana Johnson at her address in Valrico, Florida. The packages contained a total of $2,500.00 in cash. S.G. reported that he was sending money to his online girlfriend's sister who he believed to be Diana Johnson.

Grant Scam Victim K.M.

26. On December 12, 2019, a co-conspirator caused victim K.M. to send $4,000 in cash via Federal Express to Roger Johnson at the address he shared with Fenton-Johnson in Valrico, Florida. The money arrived on December 13, 2019.

27. On December 13, 2019, Diana Johnson and her co-conspirators negotiated a trade of BTC with CI#19-2002 for a counter deposit of $25,000 into bank accounts controlled within the Eastern District of Texas and directed the BTC to be deposited into 14crmboVbp4Rw73MBeA85tjuNEDMDAPaoL ("14cr").

28. Law enforcement officers contacted victim K.M. Between December 2019 and January 2020, K.M. sent four packages to Roger Johnson at the same address in Valrico, Florida. The packages contained a total of $17,450.00 in cash. K.M. reported that she was informed that she was in the process of applying for a federal grant.

Romance Scam Victim J.C.

29. On February 4, 2020, a co-conspirator caused victim J.C. to send cash via Federal Express to Diana Johnson at her address in Valrico, Florida. The money arrived on February 5, 2020.

30. On February 5, 2020, Diana Johnson and her co-conspirators negotiated a trade of BTC with CI#19-2002 for a counter deposit of $14,000 into bank accounts controlled within the Eastern District of Texas and directed the BTC to be deposited into 1KFgQE6Z7mSHTpcAb74XKzm79JrTiZ31hv ("1KFg").

31. On February 6, 2020, a co-conspirator caused victim J.C. to send cash via Federal Express to Diana Johnson at her address in Valrico, Florida. The money arrived on February 7, 2020.

32. On February 7, 2020, Diana Johnson and her co-conspirators negotiated a trade of BTC with CI#19-2002 for a counter deposit of $13,800 into bank accounts controlled within the Eastern District of Texas and directed the BTC to be deposited into 1Newa9zeagNmGmSUsrR1SFmVyx7Y5GxLM ("1New").

33. Law enforcement officers contacted victim J.C. In February 2020, J.C. sent three packages to Diana Johnson at her address in Valrico, Florida. J.C. reported that he sent approximately $30,000 to his online girlfriends. He has not met any of his online girlfriends in person.

Ogaga Michael Panama

34. The account records for PANAMA's Binance wallet were obtained. The Binance records reflect that the Binance account with user ID number 26257660 is registered to Ogaga Michael PANAMA. The records include the Federal Republic of Nigeria National driver's license bearing the name of Ogaga Michael PANAMA and the email address panmic2000@yahoo.com. The Binance account was opened on or about February 10, 2018. Records obtained from Binance also confirmed that wallet 1G8knkastmE7nQQ9eDFgP8QWpWuk4hy9Yt ("1G8k" or PANAMA's Wallet) belongs to Binance Account ID 26257660 held in the name of Ogaga Michael PANAMA. A

review of the transactional details of the account shows that at the time of this writing 1G8k has received approximately 8,141 BTC, with the majority of the BTC being sent from private wallets and peer-to-peer networks such as Localbitcoins.com. The records reflect PANAMA's Wallet has had approximately $67,000,000 U.S. dollars transferred through it since it was opened. The wallet currently has a value of approximately $430,000.00 U.S. dollars.

35. A transactional review of records obtained from Binance shows that PANAMA's Wallet activity included regular trade and internal purchase orders for alternate forms of cryptocurrency, including Tether (USDT). From the date of the account's opening to December 2020, PANAMA's Wallet conducted approximately 13,000 trade and internal purchase orders for USDT. Specifically, as part of the trade orders, PANAMA's Wallet successfully completed trades on Binance's platform to convert BTC into USDT.

36. Concerning the transactions described above with Diana Johnson, agents utilized Blockchain analysis, records from Binance, and other investigative techniques, to trace the proceeds from fraud that were traded with CI#19-2002 and USSS agents in an effort to launder the funds that were remitted to PANAMA's 1G8k Binance account at PANAMA's behest.

37. The transaction tracing for victim S.G. showed the following:

a. On November 22, 2019, at the request of Diana Johnson, CI#19-2002 remitted .2044 BTC to deposit address 13HW9yMGeEtC9JCgn8spPsPYEWK4qBZvb1 [REF TXID: 2e1719eb700eaf0934e6a822777c6a8207c8bee16036c93434ae95a694b9f516].

b. On November 22, 2019, 13HW9yMGeEtC9JCgn8spPsPYEWK4qBZvb1 remitted .2044 BTC to intermediary wallet 1FPZrU91JkUnAXBNeQegiGtSCNW3bGUkc7 [REF TXID: bb081b2e6fe100726399b59e549e6cc3a51e073b95b2744abbd1b7ee46c85bf1].

c. On November 22, 2019, 1FPZrU91JkUnAXBNeQegiGtSCNW3bGUkc7 remitted .2044 BTC to PANAMA's Wallet [REF TXID: 7768bbc2da5383b79d2f6b2f1cf74bfc13da491625e86ab7fc5941df67401fab].

38. The transaction tracing for victim K.M. showed the following:

a. On December 13, 2019, at the request of Diana Johnson, CI#19-2002 remitted 3.34 BTC to deposit address 14crmboVbp4Rw73MBeA85tjuNEDMDAPaoL [REF TXID: 5676bb64a633a7d7fe117001e6aba11bf9e09b830e7d582aa5af994234a232c5 and 55baa0d2bd39b1d2e8fdfd345ac58d50ec3b9fd2c3855c6acb0296ea3e847301].

b. On December 13, 2019, 14crmboVbp4Rw73MBeA85tjuNEDMDAPaoL remitted 3.34 BTC to

intermediary address 1FPZrU91JkUnAXBNeQegiGtSCNW3bGUkc7 [REF TXID: 85717a27c02b47d2cc312a5494df08774a7fc9d00fd202bec90984442db41e2c].

c. On December 17, 2019, 1FPZrU91JkUnAXBNeQegiGtSCNW3bGUkc7 remitted .081 BTC to PANAMA's Wallet [REF TXID: ca1c9d0e5d44e89364f606db903c54fd7f59c35c01c44b3d00262cbc4df0605c].

d. On December 19, 2019, 1FPZrU91JkUnAXBNeQegiGtSCNW3bGUkc7 remitted .1952 BTC to PANAMA's Wallet [REF TXID: 865675d68b9a48ca2716ed9f4e4e7fa9ae6bf473ec941cf2a7f6b03222aa42f2 and 24c48313fb52f25d99165bdd77b8993d535c1414ca03cf97e376edceb02d55b3].

39. The transaction tracing for victim J.C. showed the following:

a. On February 5, 2020, at the request of Diana Johnson, CI#19-2002 remitted 1.4 BTC to deposit address 1KFgQE6Z7mSHTpcAb74XKzm79JrTiZ31hv [REF TXID: c91729f02b7dc67dee69e7ae4b39f422d195392eecb77f427a511573990ef9fd].

b. On February 5, 2020, 1KFgQE6Z7mSHTpcAb74XKzm79JrTiZ31hv remitted 1.4 BTC to intermediary

wallet 1FPZrU91JkUnAXBNeQegiGtSCNW3bGUkc7 [REF TXID: ae365c000cf942b31bb6636fe6b83434b60d3a950d96dd4510f3626b1b9794b7].

c. On May 20, 2020, 1FPZrU91JkUnAXBNeQegiGtSCNW3bGUkc7 remitted 1.219 BTC to PANAMA's Wallet 1G8knkastmE7nQQ9eDFgP8QWpWuk4hy9Yt [REF TXID: 2e76d795c6db042e2c773bfc229c9eda727362a165299e99170727c58678331b].

d. On February 7, 2020, at the request of Diana Johnson, CI#19-2002 remitted 1.37 BTC to deposit address 1Newa9zeagNmGmSUsrR1SFmVyx7Y5GxLM [REF TXID: a2a1c567f6a6e7fc102b7b12fb99cde637ee03b29dffd9f789ca8da4b42ad625].

e. On February 7, 2020, 1Newa9zeagNmGmSUsrR1SFmVyx7Y5GxLM remitted 1.37 BTC to intermediary address 1FPZrU91JkUnAXBNeQegiGtSCNW3bGUkc7 [REF TXID: 3c499be7103e32c2dce74471d3fd35d1c6b22b01f890956fc2792d48d2a856f9].

f. On May 28, 2020, 1FPZrU91JkUnAXBNeQegiGtSCNW3bGUkc7 remitted 1.095 BTC to PANAMA's Wallet 1G8knkastmE7nQQ9eDFgP8QWpWuk4hy9Yt [REF TXID: 1bb220c43925161e36ba04f9e97010040118aaf91292223229d074062725a1ae].

Seizure Warrant

40. On January 15, 2021, USSS agents applied for a seizure warrant for all funds, monies, and other things of value stored in or accessible at Binance associated with user ID 26257660 in the name of Ogaga Michael Panama. United States Magistrate Judge K. Nicole Mitchell issued the seizure warrant on that date. Shortly thereafter, the warrant was executed, and Binance froze the account associated with PANAMA.

41. On or about February 25, 2021, USSS took possession of $526,370.41 in cryptocurrency from the account; the cryptocurrency was comprised of 3.0103 BTC, 1.0017 ETH, and 372,516.27 USDT.

42. On May 7, 2021, the United States and counsel for PANAMA executed a tolling agreement in which PANAMA knowingly, intelligently, and voluntarily gave up any right he may have concerning any applicable statute of limitations, including but not limited to 18 U.S.C. § 983(a)(3)(A), or by way of laches or other time limitation (whether statutory, contractual, or otherwise), to require the United States to file a complaint for forfeiture against the Seized Property and/or to obtain an indictment alleging that the Seized Property is subject to forfeiture no later than May 26, 2021 and any right he may have to seek dismissal of any complaint and/or any indictment on the ground that it was not filed or returned on or before May 26, 2021.

43. The Parties later agreed that the deadline by which the United States shall be required to file a complaint for forfeiture against the Seized Property and/or to obtain

an indictment alleging that the Seized Property is subject to forfeiture would be extended from May 26, 2021 to July 23, 2021. In July 2021, the parties extended the tolled deadline to October 23, 2021. In October 2021, the parties extended the tolled deadline to January 31, 2022.

CONCLUSION

44. I submit that this affidavit supports probable cause to forfeit 3.0103 BTC, 1.0017 ETH, and 372,516.27 USDT, associated with Binance user ID 26257660 in the name of Ogaga Michael Panama (PANAMA).

45. Based on my experience and the information herein, I have probable cause to believe that all funds, monies, and other things of value stored in or accessible at Binance associated with user ID 26257660 in the name of Ogaga Michael Panama are traceable to a money laundering transaction or were involved in a money laundering transaction and are therefore subject to forfeiture pursuant to pursuant to 18 U.S.C. § 981(a)(1)(A).

46. I also have probable cause to believe that all funds, monies, and other things of value stored in or accessible at Binance associated with user ID 26257660 in the name of Ogaga Michael Panama constitute proceeds traceable to a violation of 18 U.S.C. §§ 1341 and/or 1343 or a conspiracy to commit such offense and are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

47. Accordingly, I request the forfeiture of 3.0103 BTC, 1.0017 ETH, and 372,516.27 USDT, associated with Binance user ID 26257660 in the name of Ogaga Michael Panama (PANAMA), pursuant to 18 U.S.C. §§ 981(a) and 981(b).

48. The information contained in this Affidavit is based on my personal knowledge and what I have learned from other sources discussed herein.

49. This Affidavit does not purport to set forth all of my knowledge or investigation concerning this matter.

50. I have read the Complaint for Forfeiture concerning the Seized Property and I verify that the factual matters contained in it are true and correct.

Respectfully submitted,

Michael Dawson
Special Agent
United States Secret Service

Subscribed to and sworn before me on this the 27th day of January, 2022.

Notary Public, State of Texas

KATHY NASH
MY COMMISSION EXPIRES
NOVEMBER 8, 2025
NOTARY ID: 131345409